20. Active Directory - Exploitation

🛡️ How to Identify Attack Surfaces in Active Directory (AD)

Attack surfaces in AD refer to the various **entry points** or **vulnerabilities** that attackers can exploit. These include:

Attack Surface	Description
Users & Groups	Over-permissioned accounts, especially those in `Domain Admins` or with `SeDebugPrivilege`
Service Principal Names (SPNs)	Can be used for **Kerberoasting** attacks
Domain Controllers	High-value targets controlling AD—exploitable via DCSync, privilege escalation, etc.
GPOs (Group Policy Objects)	Misconfigured GPOs may allow privilege escalation
Shares and SMB Services	Open shares (e.g., SYSVOL, NETLOGON) may leak credentials or scripts
Trust Relationships	Misconfigured domain/forest trusts allow lateral movement
LDAP Access	Excessive read permissions may reveal sensitive structure
NTLM Authentication	Can be exploited via relay, capture, or brute-force attacks
Kerberos Protocol	Susceptible to Kerberoasting and ticket forgery

🔍 Tools to identify AD attack surfaces:

- BloodHound (SharpHound)
- ADExplorer
- PowerView
- LDAP queries
- CrackMapExec
- `Get-AD*` PowerShell cmdlets

🔐 How Kerberos Authentication Works in AD

Kerberos is a ticket-based authentication protocol used by AD. Here's a simplified flow:

1. **User Logs In**: Sends credentials to the **Authentication Server (AS)**.
2. **TGT Issued**: AS sends back a **Ticket Granting Ticket (TGT)** encrypted with the **KRBTGT** account key.

3. **Service Ticket Request**: User sends TGT to the **Ticket Granting Service (TGS)** to get a ticket for a service (e.g., file share).
4. **Access Granted**: User presents the service ticket to access the requested service.

🎯 Kerberos-Based Attacks

Attack	Description
Kerberoasting	Request service tickets for SPNs → brute-force offline → crack service account passwords.
Golden Ticket	Forge a TGT using the KRBTGT hash (full domain persistence).
Silver Ticket	Forge a service ticket using the service account NTLM hash.
AS-REP Roasting	Abuse accounts without pre-authentication to get crackable hashes.

🔧 Tools: `Rubeus`, `Impacket`, `Kerbrute`

🪪 Pass-the-Hash (PtH) and NTLM Exploitation

NTLM stores user password hashes that can be used for authentication **without needing the plaintext password**.

NTLM Exploitation Techniques:

Technique	Description
Pass-the-Hash (PtH)	Use stolen NTLM hashes to authenticate via SMB, RDP, etc.
NTLM Relay	Intercept NTLM authentication and relay to another service.
Credential Dumping	Extract hashes with tools like `Mimikatz`, `LSASS` dumps.

Mitigations: Enforce SMB signing, disable NTLM, use LAPS, restrict local admin accounts.

🏛️ Active Directory Structure Overview

Component	Description
Domain	A logical grouping of AD objects (users, computers, GPOs) with a shared database.
Domain Controller (DC)	A server that authenticates users and enforces policies. Hosts the AD database.
Forest	A collection of one or more domains that share a common schema and global catalog.

Component	Description
Trust Relationships	Links between domains/forests allowing access to resources across boundaries.
Organizational Units (OUs)	Containers to organize users, computers, and apply GPOs.

⚙️ Service Principal Names (SPNs)

- **SPNs** are unique identifiers for services running on servers.
- Format: `service/class:hostname:port`
- Example: `MSSQLSvc/sqlserver.domain.local:1433`

SPNs in Attacks:

- **Kerberoasting**:
    - Attacker finds SPNs tied to domain accounts.
    - Requests service ticket (TGS), dumps it, and cracks offline.
    - **Vulnerable SPNs**: Those tied to accounts with weak passwords.

🔧 Tools:

- `setspn -T domain -Q */*`
- `GetUserSPNs.py` (Impacket)
- `Rubeus`

📌 Summary

Topic	Key Point
Identify AD Attack Surfaces	Use tools like BloodHound, PowerView to map user rights, trust paths, and misconfigurations
Kerberos	Used for authentication; target of Kerberoasting, Golden Ticket, Silver Ticket
NTLM	Legacy protocol exploited via PtH, relay, and credential dumping
AD Structure	Domains, DCs, forests, and trusts form the backbone of identity and access control
SPNs	Identify services for Kerberoasting attacks